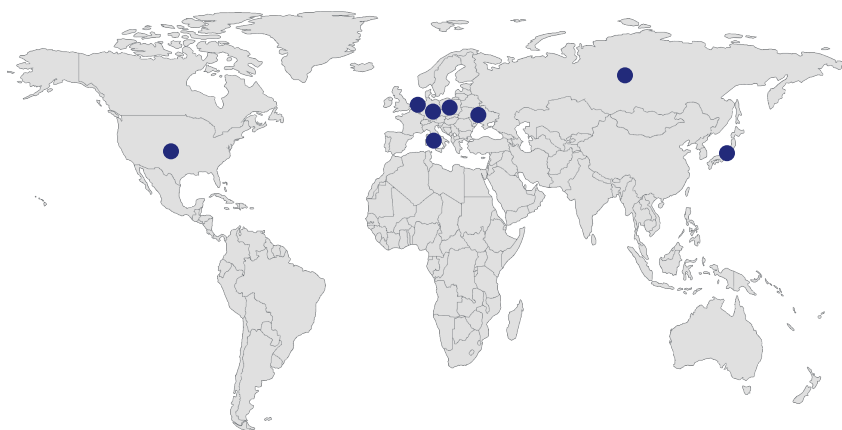


IMPERVA THREAT RESEARCH

Threat Intel Report: June 22-28, 2026

Countries



Top Tags

[FortiBleed](#)[StockStay](#)[AryStinger](#)[World Leaks](#)[ShinyHunters](#)

Executive Summary

Actionable Information:

- **Identity, access, and trusted enterprise infrastructure continue to be the highest-value targets for attackers.** FortiBleed's exposure of 86,644 verified FortiGate credentials and Russian phishing campaigns targeting Signal Backup Recovery Keys demonstrate a growing emphasis on stealing long-lived credentials that provide persistent access rather than relying solely on software exploitation. These campaigns target security appliances, encrypted communications, and authentication workflows, reinforcing that identity infrastructure remains a primary attack surface for both criminal and nation-state actors.
- **AI and software supply chains are becoming increasingly intertwined with attacker operations.** Researchers demonstrated that AI coding agents can be manipulated into executing malicious code from seemingly benign repositories, while fraudulent OpenAI workspaces targeted employees using legitimate OpenAI infrastructure. Combined with the Polymarket frontend compromise and the continued fallout from OAuth and third-party integration attacks, these incidents highlight growing risk at the intersection of AI platforms, developer workflows, cloud services, and software dependencies.
- **Nation-state operators continue expanding long-term espionage and reconnaissance capabilities rather than focusing solely on disruptive attacks.** Russian actors targeted secure communications used by government and military personnel, Turla expanded malware operations beyond Ukraine into multiple European countries, and AryStinger transformed thousands of legacy routers into covert reconnaissance infrastructure. These campaigns emphasize persistence, intelligence collection, and infrastructure positioning that can support future operations long before overt attacks occur.
- **Data breaches increasingly originate through trusted third parties, phishing, and software dependencies rather than direct compromise of primary infrastructure.** Incidents affecting Xsolis, LastPass, KDDI, Tata Electronics, and NAIC demonstrate how third-party software, OAuth integrations, phishing, and enterprise applications continue to expose large volumes of sensitive

information. Organizations managing healthcare, telecommunications, manufacturing, and financial data remain attractive targets because these sectors combine high-value identity information with complex vendor ecosystems that expand the attack surface.

Outlook:

This week's activity reinforces the continued convergence of identity theft, AI-enabled attacks, and supply-chain compromise as dominant themes across both cybercrime and nation-state operations. Attackers are increasingly leveraging trusted infrastructure—including security appliances, encrypted messaging platforms, AI development tools, SaaS integrations, and software dependencies—to obtain persistent access while minimizing opportunities for detection. At the same time, law enforcement successes such as Operation Endgame demonstrate that coordinated international disruption can significantly degrade malware ecosystems, although threat actors continue replacing lost infrastructure with more resilient, decentralized alternatives. Organizations should expect continued targeting of credential stores, developer environments, AI workflows, and third-party integrations, making identity protection, privileged access management, vendor risk oversight, and behavioral monitoring increasingly critical components of enterprise cyber defense.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

5,779% [CVE-2026-1492](#)

- The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to improper privilege management in all versions up to, and including, 5.1.2. This is due to the plugin accepting a user-supplied role during membership registration without properly enforcing a server-side allowlist. This makes it possible for unauthenticated attackers to create administrator accounts by supplying a role value during membership registration.

533% [CVE-2026-42945](#)

- NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, \$1, \$2) with a replacement string that includes a question mark (?). An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

459% [CVE-2026-21962](#)

- Vulnerability in the Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware (component: Weblogic Server Proxy Plug-in for Apache HTTP Server, Weblogic Server Proxy Plug-in for IIS). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in. While the vulnerability is in Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data. Note: Affected version for Weblogic Server Proxy Plug-in for IIS is 12.2.1.4.0 only. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).

Recent Cyber Threats

FortiBleed Harvests FortiGate Credentials at Global Scale

+FortiBleed +Russia

- A Russian-speaking initial access broker was linked to [FortiBleed](#), a credential-harvesting operation targeting more than 430,000 FortiGate firewalls globally. Reporting found 86,644 verified working credentials across 194 countries, with generic admin accounts, Fortinet built-in accounts, and organization-specific accounts all represented. The campaign reportedly involved more than 1.16 billion credential attempts and highlights continued attacker focus on firewall and VPN credentials as direct enterprise access paths.

Russian Actors Target Signal Backup Recovery Keys

+Russia +Phishing +Government +Ukraine +US

- The FBI and CISA warned that [Russian intelligence-linked](#) actors expanded phishing campaigns against Signal users to steal Backup Recovery Keys, potentially exposing historical messages rather than only current account access. The campaign targets high-intelligence-value individuals, including U.S. and international officials, military personnel, political figures, journalists, and Ukraine-linked targets. Attackers continue impersonating messaging-platform support services and are tracked publicly as UNC5792 and UNC4221.

Turla Deploys StockStay Malware Against Ukraine

+StockStay +Turla +Ukraine +Italy +Netherlands +Poland +Germany

- Researchers detailed [StockStay](#), a Turla malware strain under development since at least December 2022 and used primarily against Ukrainian government and defense targets. StockStay shares code and functionality with Kazuar, and Turla used phishing emails with malicious RDP configuration files to connect victim systems to attacker infrastructure. The malware has also appeared in Italy, the Netherlands, Poland, and Germany, indicating broader European targeting beyond Ukraine.

AI Coding Agents Tricked Into Running Malware From Clean Repos

+AI +Malware

- Researchers recently demonstrated an attack where a clean-looking GitHub repository can cause an AI coding agent such as Claude Code to execute a [malicious payload](#) without obvious exploit code in the repo itself. The chain relies on normal setup instructions, a package initialization error, and a shell script that retrieves attacker-controlled commands from DNS TXT records. Successful exploitation gives the attacker a shell running with developer privileges, exposing environment variables, API keys, and local configuration files.

Fraudulent OpenAI Tenants Target Cybersecurity Firms

+AI +Phishing

- Threat actors created [OpenAI](#) organizations impersonating legitimate companies and sent employees real OpenAI tenant invitations from OpenAI's legitimate notification infrastructure. Push Security found the campaign after employees received invites to a fake "Push Security Inc." workspace controlled by Gmail accounts, with similar activity also targeting other cybersecurity and technology companies. The objective appears to be tricking employees into entering sensitive corporate data into attacker-controlled ChatGPT workspaces and projects.

Polymarket Users Lose \$3 Million in Frontend Supply-Chain Attack

+Crypto +Supply-chain

- [Polymarket](#) said it will reimburse users after attackers injected malicious JavaScript into the platform frontend through a compromised website dependency. The script tricked users on the official site into approving fraudulent transactions, while Polymarket said its backend infrastructure was not impacted. Blockchain firms estimated roughly \$3 million was stolen from fewer than 15 accounts and later bridged from Polygon to Ethereum and swapped into about 1,893 ETH.

Amadey and StealC Malware Infrastructure Disrupted

+Amadey +StealC

- [Operation Endgame](#) disrupted infrastructure supporting Amadey and StealC, two malware ecosystems used for credential theft, payload delivery, and broader cybercrime enablement. The coordinated action involved Microsoft, Europol, Bitdefender, Bitsight, ESET, and other partners, and reportedly recovered 27 million stolen credentials. The takedown targeted malware infrastructure that supports ransomware and fraud operations rather than a single isolated campaign.

AryStinger Builds Recon Proxy Network From Legacy Routers

+AryStinger +Malware +Botnet

- Researchers reported [AryStinger](#), a malware family infecting at least 4,300 legacy routers to build a reconnaissance and proxy network rather than a conventional DDoS botnet. The campaign turns neglected edge devices into distributed infrastructure for scanning and anonymized activity. The activity reflects continued attacker interest in SOHO and legacy router compromise as low-noise infrastructure for reconnaissance, proxying, and follow-on operations.

Data Breaches

KDDI Breach Exposes Up to 14.2 Million ISP Email Logins

+Japan +Telecommunications

- Japanese telecom operator [KDDI](#) disclosed that attackers accessed an email system used by five other ISPs, potentially exposing email addresses and passwords for up to 14.2 million current, former, and inactive accounts. KDDI discovered the compromise on June 17 and said attackers exploited a vulnerability in unnamed third-party software. Some passwords were stored hashed or encrypted, but KDDI did not specify the encryption type or how many accounts may have had plaintext passwords exposed.

Xsolis Breach Impacts Nearly 1.4 Million Healthcare Records

+Healthcare +AI

- Healthcare technology company [Xsolis](#) disclosed that a targeted phishing attack gave attackers access to files containing sensitive customer information for 1,396,519 people. Exposed data included names, addresses, dates of birth, health insurance information, Social Security numbers, and medical treatment information. Xsolis provides AI-powered software used by more than 600 hospitals and health insurers for utilization management, medical necessity reviews, discharge planning, and reimbursement decisions.

LastPass Salesforce Data Exposed Through Klue Supply-Chain Attack

+Supply-chain +OAuth

- [LastPass](#) confirmed that attackers used OAuth tokens stolen from Klue to access support cases and customer data in its Salesforce environment. Exposed data may include customer names, phone numbers, email addresses, physical addresses, support case information, and sales or CRM-related data, though LastPass said vaults, products, services, and core infrastructure were not affected. The incident shows how OAuth token compromise at a third-party integration can expose downstream customer data across multiple SaaS environments.

Tata Electronics Confirms Cyberattack After Supplier Documents Leak

+Electronics +World Leaks

- [Tata Electronics](#) confirmed a cybersecurity incident affecting some systems after World Leaks claimed it published confidential client documents. Researchers reviewing samples said the leaked material may include Apple supplier specifications and Tesla-related manufacturing documents, though the authenticity of the data was not independently verified. Tata said operations were unaffected but did not disclose whether data was stolen, whether it received a ransom demand, or the full scope of the breach.

NAIC Confirms PeopleSoft Breach Linked to ShinyHunters Claims

+ShinyHunters +Supply-chain

- The [National Association of Insurance Commissioners](#) confirmed a cyberattack exploiting an Oracle PeopleSoft zero-day, while ShinyHunters claimed it stole about 3.1 TB of data. NAIC said the stolen information included publicly available statutory financial reports, insurer investment credit rating data, and technical information such as outdated logs and configuration files, with no evidence that personal, banking, or payment data was accessed. ShinyHunters claimed a broader cache including insurer filings, credit rating files, AWS logs, cloud configs, and PII, and the leaked files suggest NAIC did not pay.

Bajaj Auto Reports Ransomware Attack on Internal Systems

+Automotive +Ransomware

- [Bajaj Auto](#) disclosed a ransomware attack affecting systems at the parent company and its wholly owned subsidiary Bajaj Auto Technology Ltd. The incident occurred around 8 a.m. IST on June 23, and the company said technical teams, cybersecurity experts, and management initiated response protocols to contain and mitigate impact. Bajaj said mitigation measures were successful based on available information but did not disclose the extent of disruption, whether data was compromised, or whether manufacturing operations were affected.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs— including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.